IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA, Plaintiff, vs. DANIEL STRATMAN, Defendant.	**4:13CR3075** **FINDINGS, RECOMMENDATION AND ORDER**

This matter is before the court on Defendant's Motion to Dismiss Counts I and II of the Indictment, (Filing No. 6). For the reasons set forth below, the motion to dismiss should be denied.

BACKGROUND

A twelve-count indictment was filed against Defendant Daniel Stratman on June 19, 2013. Counts I and II of the Indictment allege Stratman violated 18 U.S.C § 1030(a)(5)(A) on May 23rd and May 24th. Specifically, the Indictment alleges:

> DANIEL STRATMAN, knowingly caused the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to a protected computer, to wit, the University of Nebraska and Nebraska State College Systems computer systems, and the offense caused loss to a person or persons during a 1-year period, from the defendant's course of conduct affecting a protected computer, aggregating at least $5,000 in value.
>
> In violation of 18 U.S.C. § 1030(a)(5)(A) and (c)(4)(B).

Filing No. 1, at CM/ECF pp. 1-2.

Defendant alleges that because Defendant's initial access to the Nebraska State College Systems computer system was authorized "he could not have committed the offenses in Counts I and II, as a matter of law." (Filing No. 15, at CM/ECF p. 3).

ANALYSIS

"An indictment is legally sufficient on its face if it contains all of the essential elements of the offense charged, fairly informs the defendant of the charges against which he must defend, and alleges sufficient information to allow a defendant to plead a conviction or acquittal to bar a subsequent prosecution." United States v. Fleming, 8 F.3d 1264, 1265 (8th Cir. 1993). The defendant argues the Indictment is defective because it fails to include an essential element of the offense; specifically, he claims any charge against him for violating 18 U.S.C. § 1030(a)(5)(A) must allege Stratman was not "permitted initial authorized access" to the University computer system.

To resolve the defendant's motion, the court must determine the meaning of 18 U.S.C. § 1030(a)(5)(A) and the elements required to prove it was violated. "If the plain language of [a] statute is unambiguous, that language is conclusive absent clear legislative intent to the contrary. Therefore, if the intent of Congress can be clearly discerned from the statute's language, the judicial inquiry must end." United States v. McAllister, 225 F.3d 982, 986 (8th Cir. 2000). "When the statutory language is plain, the sole function of the courts – at least where the disposition required by the text is not absurd – is to enforce it according to its terms." Arlington Cent. Sch. Dist. Bd. of Educ. v. Murphy, 548 U.S. 291, 296 (2006)(internal quotation marks omitted).

18 U.S.C. § 1030(a)(5)(A) provides: "Whoever . . . knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer . . ." is subject to punishment under other provisions of the Consumer Fraud and Abuse Act ("CFAA"). Stratman argues the statutory phrase "intentionally causes damages without authorization" must be interpreted to mean the statute applies to only those individuals who initially accessed the computer without permission; "without authorization" cannot

modify the word "damages" because "who would be authorized to cause damage?" (Filing No. 15, at CM/ECF p. 2).

As defined in the CFAA, "damage" is "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Under this definition an individual could cause "damage" to a protected computer by merely deleting files or taking a network offline to install upgrades. Both of those tasks would certainly "impair the availability of data, a program, a system, or information." However, Information Technology professionals are undoubtedly authorized to "damage" – as defined by 1030(e)(8) – computer systems as part of their daily tasks. Likewise, an employee who deletes files is impairing the availability of data, but may be authorized to do so. The definition of damage does not distinguish between unauthorized or authorized "damage," thus the modifier "without authorization" is necessary in the text of 1030(a)(5)(A). Contrary to the defendant's argument, the phrase "without authorization" modifies the phrase "intentionally causes damage," and not access to the computer itself.

The foregoing interpretation has been adopted by the courts. In International Airport Centers, LLC v. Citrin, 440 F.3d 418, 421 (7th Cir. 2006),[1] a former employee argued that under his employment contract, he was authorized to use his laptop computer, and therefore did not violate § 1030(a)(5)(A) by destroying data on the laptop "without authorization" after he was no longer employed. However, the court drew a distinction between authorized damage and unauthorized damage, concluding "it is unlikely, to say the least, that the provision was intended to authorize" post-employment data destruction when the company had no duplicates of information destroyed. Citrin, 440 F.3d at 421.

[1] The Citrin court also discussed the distinction between the terms "without authorization" and "exceeds access" but did not rely on that distinction in discussing Citrin's possible violation of 1030(a)(5)(A). Rather the court engaged in that discussion in the context of a possible violation of what is now 18 U.S.C. § 1030(a)(5)(B) – a section that is not at issue in this motion to dismiss.

See also,[2] KLA-Tencor Corp. v. Murphy, 717 F. Supp. 2d 895, 903-04 (N.D. Cal. 2010)(noting whether contract authorized employees to delete confidential files was a key issue to determine liability under CFAA); In re America Online, Inc. 168 F. Supp. 2d 1359, 1371 (S.D. Fla. 2001)(quoting legislative history stating 1030(a)(5)(A) was intended to punish anyone who intentionally damages a computer); Condux Intern., Inc. v. Haugum, case no. 08-4824, 2008 WL 5244818 at *6-7 (D. Minn. Dec. 15, 2008)(1030(a)(5)(A) does not require unauthorized access to a computer, rather it is based on unauthorized damage); B & B Microscopes v. Armogida, 532 F. Supp. 2d 744, 758 (W.D. Penn. 2007)(1030(a)(5)(A) is predicated on unauthorized damage to a computer, not unauthorized access); Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 967 n. 1 (D. Ariz. 2008)(violation of 1030(a)(5)(A) defined by causing damage without authorization). But see Advanced Aerofoil Tech., AG v. Todaro, case no. 11cv9505, 2013 WL 410873 at *8 n. 3 (S.D.N.Y. Jan. 30, 2013)(finding, without discussion, that the phrase "without authorization" must modify the "conduct of 'knowingly causes the transmission' " because the word "damage" in 1030(a)(5)(A) "presupposes the conduct causing damage was not authorized").[3]

The indictment against Stratman mirrors the language of the 18 U.S.C. § 1030(a)(5)(A). It need not allege the defendant's use of the university computer was unauthorized. 18 U.S.C. § 1030(a)(5)(A) is violated if a defendant, without authorization, intentionally impairs the integrity or availability of data, a program, a system, or information held within (i.e. "damages") a computer. Defendants' motion to dismiss should be denied.

---

[2] These cases discuss the interpretation in the context of a civil cause of action, which is expressly allowed by 18 U.S.C. § 1030. But this distinction does not make a difference for the interpretation of the plain language of the statute. Additionally, these cases often cite to prior versions of the statute – 1030(a)(5)(A) was previously 1030(a)(5)(A)(i). However, the requirement of finding damage caused without authorization has remained unchanged.

[3] The court respectfully disagrees with the Advanced Aerofoil Tech. court's statement that "damage" presupposes that the conduct causing the damage was unauthorized. As explained supra, as defined by 1030(e)(8), various types of "damage" could be authorized.

Accordingly,

IT THEREFORE HEREBY IS RECOMMENDED to the Honorable John M. Gerrard, United States District Judge, pursuant to 28 U.S.C. § 636(b), that the motion to dismiss filed by the defendant (Filing No. 6) be denied in its entirety.

The defendant is notified that failing to file an objection to this recommendation as provided in the local rules of this court may be held to be a waiver of any right to appeal the court's adoption of the recommendation.

IT IS ORDERED, that the defendants request for a hearing on the motion to dismiss be denied.

Dated this 5th day of August, 2013.

BY THE COURT:

s/ Cheryl R. Zwart
United States Magistrate Judge